REMARKS

Applicant respectfully requests reconsideration and allowance of all of the claims of the application. The status of the claims is as follows:

- Claims 1, 9, 12, 15, 17, 19 and 21-24 are pending.

Cited Documents

The following documents have been applied to reject one or more claims of the Application:

- **Hamann:** Hamann et al., U.S. Patent Application Publication No. 2002/0026578
- **Dancs**: Dancs, U.S. Patent No. 6,108,789
- **Skomora:** Skomora, U.S. Patent Application Publication No. 2005/0076198
- **Palaniswany**: Palaniswany, U.S. Patent No. 6,751,095

Claims 1, 9, 12, 15, 17, 19 and 21-24 are Non-Obvious over Hamann, Dancs, Skomora and Palaniswany

Claims 1, 9, 12, 15, 17, 19 and 21-24 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Hamann, Dancs, Skomora and Palaniswany. Applicant respectfully traverses the rejection.

Independent Claim 1

Claim 1 recites, in part (emphasis added):

> **reading said root certificate from said smartcard memory**;
>
> **storing said root certificate in a computer memory of a computing device**, the computing device operatively coupled to said smartcard, wherein the storing comprises copying said root certificate from the smartcard to a certificate store maintained in said computer memory;
>
> ...
>
> **erasing said root certificate from said computing device operatively coupled to said smartcard** in response to determining that said smartcard is no longer operatively available.

1. The documents of record do not teach or suggest "reading" a root certificate from a smartcard.

Applicant respectfully submits that "reading said root certificate from said smartcard memory" is a novel and non-obvious act that is not taught or suggested by the documents of record, singly and in combination(s). Applicant respectfully submits that none of the documents of record disclose any way to read a root certificate, *i.e.*, to obtain a copy of the root certificate such that it may be stored to a computer memory of a computer coupled to the smartcard. Known smartcard security systems work by putting a root certificate into the smartcard. Once inside the smartcard, the root certificate can be used to digitally sign something, and to thereby prove that the root certificate does, in fact, reside within the smartcard. However, known systems do not provide a means to read the certificate (or determine its nature) once it is inside the smartcard.

Thus, the root certificate, in the documents of record, is not read from the smartcard memory. Instead, smartcards described in the documents of record perform calculations inside the smartcard to indirectly prove that the root certificate resides within the smartcard. Such an indirect proof proves, without removing the root certificate for examination, that the root certificate is present. Such a proof avoids loss of the nature (specific digits) of the root certificate into common knowledge.

Thus, the documents of record actually teach away from reading the certificate out of the smartcard. In particular, Hamann suggests, at paragraph 0025 (emphasis added):

> A cryptographical processor as used by the present invention is needed for performing signature operations **on the card itself**. The user's private key **never needs to leave the smart card**.

The Hamann document was cited as alleged disclosing reading a root certificate from a smart card. The Office suggests (at the center of page 3 of the Action mailed 04/15/2011) that paragraph 0039 of Hamann discloses reading a root certificate from a smartcard. Applicant respectfully disagrees.

In fact, paragraph 0039 describes actions taking place inside the smartcard. As described above, a digital signature created by a smartcard can indirectly prove that the root certificate is inside the smartcard without removal of that root certificate. Thus, what Hamann is doing in paragraphs 0034 to 0042 is explained by the last sentence of paragraph 0033. In particular, Hamann discloses that: "A new user certificate is only accepted by the smart card when the digital signature of the certificate provided with the certificate is successfully verified on the card using the public root key of the CA." Thus,

Hamann discloses that the smartcard is verifying the digital signature in a manner that uses the public root key of the Certificate Authority (CA).

Accordingly, Hamann discloses conventional technology, wherein the root certificate is locked into the smartcard, and cannot be read out of the smartcard. Its existence inside the smartcard is determined indirectly, however, by the root certificate's ability to sign documents by operation within the smartcard.

Hamann, at paragraph 0039, discloses step 5 in an algorithm, which states:

> 5. Verifying the digital signature contained in the new user certificate and using the public root key stored in EEPROM for decrypting the digital signature (50).

Applicant respectfully submits that the "verifying" step of paragraph 0039 is actually a calculation in the smartcard, and is not a "reading" step. That is, there is no reading of data from the smartcard in a manner that allows the data to be stored in a computer operatively coupled to the smartcard.

Instead, there is a calculation to verify that the signature was signed by the private key associated with the public key. That is, the calculation decrypts the signature using the public key, to "verify" that it is valid, *i.e.*, that it was encrypted by the party associated with the public key.

Not only is the "verifying" step not a "reading" step, but Hamann's paragraph 0039 also does not mention a "root certificate," as recited by claim 1. Neither the "digital signature" nor the "public root key," mentioned in Hamann's paragraph 0039, is a root certificate. The public key is by its very nature freely (publicly) available, and quite different from a root certificate, which is a guarded data element. The digital signature

is also not a "root certificate." The digital signature is data produced by the private key, and may be decrypted by the public key. Accordingly, Applicant respectfully submits that Hamann does not teach or suggest "reading said root certificate from said smartcard memory," as recited by claim 1.

The Dancs document was cited as allegedly disclosing a password requirement. At column 7 lines 23-40, Dancs describes a client device that checks to see if a smart card is inserted in a slot. Upon detection of the smartcard, the user is challenged for a PIN or password. However, the Office does not suggest that Dancs teaches or suggests the "reading" step of claim 1. Moreover, Applicant respectfully submits that Dancs does not teach or suggest "reading said root certificate from said smartcard memory," as recited by claim 1.

The Skomra document was cited as determining if a smartcard is no longer operatively available to the computing device. At paragraph [0114], Skomra describes that removal of a smartcard means that the user endpoint device no longer has the signed user's certificate, and therefore is an unauthorized user endpoint device. However, the Office does not suggest that Skomra teaches or suggests the "reading" step of claim 1. Moreover, Applicant respectfully submits that Skomra does not teach or suggest "reading said root certificate from said smartcard memory," as recited by claim 1.

The Palaniswamy document was cited as disclosing erasing of a root certificate. However, the Office does not suggest that Palaniswamy teaches or suggests the "reading" step of claim 1. Moreover, Applicant respectfully submits that Palaniswamy

does not teach or suggest "reading said root certificate from said smartcard memory," as recited by claim 1.

2. The documents of record do not teach or suggest "storing" a root certificate into a computer operatively coupled to a smartcard.

Applicant respectfully submits that "storing said root certificate **in a computer memory of a computing device**, (emphasis added)" is a novel and non-obvious act that is not taught or suggested by the documents of record, singly and in combination(s). Instead, at most, the documents of record disclose **storing a root certificate in a smartcard, and not on a computer attached to the smartcard**.

In the middle of page 3 of the Office Action, the Office suggests that paragraph 0032 of Hamann discloses storing a root certificate in a computer coupled to a smartcard. Applicant respectfully submits that the storing is actually performed on the smartcard, and not on the computer attached to the smartcard. This is significant, because it indicates that the root certificate is stored on the smartcard, and not the computer, as recited by claim 1.

Referring to Hamann at paragraph 0032, Harmann explicitly states: "The new user certificate is returned by the CA to the user's client system **and is then stored on the smart card** (emphasis added)." Thus, Hamann discloses the typical technology involving storage of a certificate on the smartcard. In contrast, Applicant's claims recite "reading said root certificate from said smartcard memory" and "storing said root certificate in a computer memory of a computing device."

Applicant respectfully submits that Palaniswamy similarly fails to teach or suggest "storing said root certificate in a computer memory of a computing device." Instead, Palaniswamy describes storage and/or deletion of a root certificate residing on a smartcard and/or SIM (subscriber identity module). Referring to Palaniswamy at column 3, lines 34-53, Palaniswamy discloses storage (line 38) and the use of a SIM, which is a smartcard device (line 52). Accordingly, Palaniswamy discloses saving a certificate onto a SIM (smartcard), and fails to teach or suggest "storing said root certificate in a computer memory of a computing device," as recited by claim 1.

Danes and Skomra are not cited by the Office, and fail to address the "storing" step.

3. The documents of record do not teach or suggest "erasing" a root certificate from said computing device operatively coupled to said smartcard.

Applicant respectfully submits that "**erasing said root certificate from said computing device operatively coupled to said smartcard**, (emphasis added)" is a novel and non-obvious act that is not taught or suggested by the documents of record, singly and in combination(s). Instead, at most, the documents of record disclose erasing a certificate from a smartcard. The documents of record to not teach or suggest erasing **a certificate on a computer attached to the smartcard**.

The Office points to Palaniswamy at columns 3, 6 and 7, and suggests that Palaniswamy discloses erasing a root certificate from a computing device operatively connected to a smart card.

However, Applicant respectfully submits that Palaniswamy discloses erasure of a certificate from a smartcard. In particular, Palaniswamy discloses erasure of a certificate from a SIM module. A SIM module is a Subscriber Identity Module (column 1, line 25) which is a smartcard (column 4, line 43). **Thus, Palaniswamy discloses erasure from a smartcard and not from a computer attached to a smartcard, as recited by claim 1**.

For at least the reasons presented herein, the combination of Hamann, Danes, Skomra and Palaniswamy does not teach or suggest all of the features of claim 1. Accordingly, Applicant respectfully requests that the Office withdraw the § 103 rejection of claim 1.

Independent Claims 9, 17, 21 and 23

Claims 9, 17, 21 and 23 are allowable for at least the reasons claim 1 is allowable. The remarks from above are incorporated herein by reference.

Accordingly, Applicant respectfully requests that the Office withdraw the § 103 rejection of claims 9, 17, 21 and 23.

Dependent Claims 12, 19, 22 and 24

Claims 12, 19, 22 and 24 ultimately depend from independent claims 9, 17, 21 and 23, respectively. As discussed above, claims 9, 17, 21 and 23 are allowable over the cited documents. Therefore, claims 12, 19, 22 and 24 are also allowable over the cited documents of record for at least their dependency from an allowable base claim,

and also for the additional features that each recites.

Accordingly, Applicant respectfully requests that the Office withdraw the § 103 rejection of claims 12, 19, 22 and 24.

Conclusion

For at least the foregoing reasons, all pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application.

If any issues remain that would prevent allowance of this application, **Applicant requests that the Examiner contact the undersigned representative before issuing a subsequent Action.**

Respectfully Submitted,

Lee & Hayes, PLLC
Representative for Applicant

/David S. Thompson 37954/ Dated: 15 July 2011

David S. Thompson
(davidt@leehayes.com; 509-944-4735)
Registration No. 37954

David A. Divine
(Daved@leehayes.com; 509-944-4733)
Registration No. 51275